جامعة دمشق

كلية الهندسة المعلوماتية

قسم النظم و الشبكات الحاسوبية



Network Security

WiFi

إعداد :

م. مصطفى محمد نجم

مقدمة :

لم يكن الوقت بعيداً حينما كان استخدام الحاسب الآلي مقصوراً على قله من المهتمين الذين يملكون مالاً كافياً لشرائه. فسعر جهاز الحاسب الآلي كان مرتفعاً لدرجه أن امتلاكه أصبح من مظاهر الترف الذي يسعى لها ثلة من الميسورين ، في حين أن امتلاك شبكة بيانات كان مقصوراً على الشركات الكبيرة والكبيرة فقط .

أما الآن الوضع بات مختلفاً، فاستخدام الحاسب الآلي بات شائعاً لشريحة كبيره من المجتمع ، بل أن وجوده في المنازل صار ضرورة في أحيان كثيرة. كما انتشرت شبكات البيانات الرقمية وتعدت حاجز الشركات الكبيرة لتصل إلى المنازل أيضا. يختلف استخدام هذه الشبكات باختلاف اهتمامات المستفيدين منها ، فالبعض منها صمم من أجل المشاركة في خط الانترنت ومنها من يتعدى ذلك إلى المشاركة في الملفات بين الأجهزة الموجودة داخل الشبكة الواحدة مستفيداً من السرعة العالية التي توفرها هذه الشبكات.

ومع تقدم العلم في مجال الشبكات اللاسلكية وتوفرها بأسعار معقولة جعل إقبال الناس عليها جيد جدا في الفترة الأخيرة وخصوصاً أنها تكفيهم مشكله الأسلاك المتدلية بين أجهزة الشبكة الواحدة. حيث أن الحصول على شبكه لاسلكية ليس بالأمر الصعب، فهو لايتطلب سوى الحصول على مودم يتوفر به موزع شبكه لاسلكية بجانب وجود أجهزة حاسب آلي متوفر بها كرت شبكه لاسلكية. لكن إستخدام هذه النوعيه من الشبكات قد يجلب مشاكل لا تجلبها الشبكات التقليدية ذات الكبلات (السلكية). حيث أن الشبكات اللاسلكية تعتمد في نقلها للبيانات على ذبذبات ترسلها في الهواء . هذه الذبذبات من السهل التقاطها والإطلاع على محتوياتها ومن ثم العبث بها.

وجود هذه المشاكل لا يعني إطلاقاً عدم استخدام هذه النوعية من الشبكات ولكن يجب أن نكون أكثر حذراً ونفكر كيف من الممكن منع المتطفلين من الدخول إلى هذه النوعية من الشبكات ، أو بعبارة أخرى ، هي كيف نحمي شبكتنا اللاسلكية

صناعة الشبكات اللاسلكية من أسرع الصناعات تطورا في عالم الشبكات وخصوصا لدى المستخدمين ذوي نطاق محدود مثل استخدامها في المنازل والشركات الصغيرة بالرغم من قصورها من الناحية الأمنية.وهذه التقنية في تطور مستمر من حيث السرعة وسعة النقل كذلك من النواحي الأمنية.ومع كل هذا التطور مازال هناك الكثير من الشركات الكبرى لديها الكثير من المخاوف في استخدام هذه التقنية وذلك لسبب قصورها من الناحية الأمنية والخطر الذي سوف تتعرض له الشركات أثناء استخدامها.

بدأت الشبكات اللاسلكية بالانتشار ومن ضمنها شبكات الواي فاي (Wireless Fidelity Wi-Fi) بصورة ملحوظة و غير متوقعة ، حتى لا تكاد تذهب إلى مكان ما إلا وتجد علامة تشير إلى وجود خدمة (Wi-Fi) ، وتوقعت دراسة حديثة نمو عدد مستخدمي نقاط الاتصال اللاسلكي في العالم من ٩,٣ ملايين مستخدم خلال العام ٢٠٠٤ ليصل إلى نحو ٣٠ مليوناً بنهاية العام الجاري. وشهدت نقاط الاتصال اللاسلكي انتشاراً واسعاً على مدى السنوات القليلة الماضية من بضع مئات خلال العام ٢٠٠٠ لتصل إلى حوالي ٤٠,٠٠٠ نقطة اتصال ساخنة في العالم خلال العام ٢٠٠٤. فما هي

(Wi-Fi) ؟ ، و بما أنها شبكة فهذا يعني أنها عرضة لتهديدات أمنية فما هي سبل الحماية ؟ هذا ما سنناقشه ضمن هذا البحث.

تعريف

(Wi-Fi) هي الشبكات اللاسلكية قصيرة المدى المكونة من مجموعة من الأجهزة المرتبطة مع بعضها البعض لتبادل المعلومات و الاستفادة من الموارد (أو المنافع) الموجودة في الشبكة من خلال وسط تراسلي لاسلكي –على الهواء–و ذلك يعطي حرية تنقل الأجهزة المرتبطة بها مادامت داخل نطاق الشبكة ، لكن مقابل هذه الميزة يظهر خطر أمني يهدد هذا النوع من الشبكات ألا وهو انكشاف البيانات المرسلة على الهواء و بالتالي تكون عرضة للاختراقات وغيرها من التهديدات الأمنية.

المعايير القياسية للشبكات اللاسلكية

ثلاثة أجيال من المعايير القياسية للشبكات اللاسلكية ظهرت حتى الآن ، وهي على التسلسل الزمني 802.11g,802.11a,802.11b وكان التركيز على سرعة أكبر لنقل البيانات ، و لم تأخذ هذه الأجيال الثلاثة الموضوع الأمني بشكل كافي مما ساعد على كون الشبكات اللاسلكية عرضة أكثر للتهديدات الأمنية. IEEE وهي الجمعية العلمية المصدرة لهذه المعايير القياسية تعمل على إصدار معيار قياسي جديد خاص بأمن الشبكات اللاسلكية و هو 802.11i و التي لم تغطها المعايير السابقة .

روتوكول	رعة	ردد
802.1	ميغابت/ث	2 غيغاهيرتز
802.1	ميغابت/ ث	غيغاهيرتز
802.1	ميغابت/ ث	2 غيغاهيرتز

مصطلحات مهمة في الشبكة اللاسلكية

- نقطة الاتصال (Access Point) : مركز استقبال و إرسال الإشارات اللاسلكية ، ومدى الشبكة اللاسلكية بحسب قوة إرسال الإشارة الصادرة من هذه النقطة.
- معرف الشبكة اللاسلكية (SSID) : اسم الشبكة اللاسلكية ، و عن طريقها يتم تعريف الشبكة اللاسلكية و الاتصال بها.
- مفتاح الحماية (WEP ،WPA): خياران للحماية بتشفير البيانات المرسلة في الشبكات اللاسلكية بحيث فقط المصرح لهم الاتصال بالشبكة بإمكانهم معرفة البيانات المرسلة بينما الملتقطين للإشارات اللاسلكية الغير مصرح لهم لا يمكنهم معرفة البيانات المرسلة . و نظام التشفير WPA أفضل بكثير من النظام WEP لكن ليس جميع الأجهزة تدعمه ، و النسخة الأمنية الجديدة من المعايير القياسية للشبكات اللاسلكية802.11i تعزز الجانب الأمني عن طريق تطوير نظام WPA وبالتالي سيكون هناك نظام مطور للتشفير وهو WPA2 .

§ النقاط الساخنة (Hotspots): عبارة عن جهاز هوائي موصول بالإنترنت ويتصل لاسلكيا مع أجهزة الحاسب في مداه الذي قد يصل إلى ٤٥ مترا، ولاتصال جهاز الحاسب بشبكة الواي فاي لابد من تهيئته لدعم هذه التقنية، ومعظم الأجهزة المحمولة التي تباع الآن مزودة بداخلها ببطاقات واي فاي. و النقاط الساخنة هي التعبير المتداول لنقاط الاتصال.

➢ WEP "Wired Equivalent Privacy":

طريقة تستخدم في تشفير البيانات المتنقلة داخل شبكة لاسلكية وذلك لمنع المخترقين من الحصول على البيانات.

وتستخدم مفتاح سري مشترك "Shared Secret Key" لجميع المستخدمين المكون من ٤٠ بت أو ١٠٤ بت والذي يضاف إليه القيمة الابتدائية " Initial Vector" وهو عبارة عن ٢٤ بت. والشائع استخدامه هو ١٠٤ بت "١٢٨ بت"ويعتمد على خوارزمية تشفير تسمى "RC4".

عيوبها:

بعد انتشار استخدامها قامت بحوث ودراسات هدفها كشف عيوب الـ WEP ومنها:

- استخدامها لمفتاح سري مشترك يتم توزيعه يدويا على جميع المستخدمين مما يجعل عملية التغير متعبة وخصوصا في الشركات الكبرى مما يمد في عمر المفتاح السري المشترك وبالتالي يسهل عملية الاختراق وكشف المفتاح.
- قصر طول المفتاح مما يجعل اكتشاف المفتاح مهمة سهلة للمخترقين.
- رأس حزمة البيانات المرسلة غير مشفر مما يتيح معرفة عنوان المرسل والمستقبل وذلك يسهل عملية المخترقين في معرفة المفتاح.

مما يجعل استخدامه غير ملائم لفئة الشركات الكبرى وهو مناسب لمستخدمي المنازل والمؤسسات.

➢ WPA "Wi-Fi Protected Access":

هي عبارة عن برنامج "Firmware" صمم لتصحيح عيوب الـ WEP يحمل على الأجهزة المستخدمة (نقاط الوصول "AP" أي لا يتطلب تغيرها وهو مرحلة انتقاليه أو وسيطة بين ال WEP و 802.11i ويزيد من مستوى حماية البيانات وكذلك في التحكم في الدخول إلى الشبكة اللاسلكية حيث لا يسمح إلا للأشخاص المصرح لهم مما يجذب الشركات الكبرى إلى استخدامه.

بالنسبة للاستخدام في الشركات يتطلب وجود خادم للشبكة للتحقق من هوية المستخدم "Authentication Server" من نوع 802.1x مع EAP برتوكول.

أما لمستخدمي المنازل والمؤسسات الصغيرة ليس هناك حاجة إلى توفر خادم الشبكة " Authentication Server" كل ما على المستخدم عمله هو إدخال المفتاح السري " Pre-shared Key" أو الرقم السري على جهازه الذي يريد من

خلاله الدخول على الشبكة. لكل مستخدم رقم سري خاص به هو الذي يحدد هويته ومدى الصلاحيات المقدمة لهذا المستخدم وهو بعكس ال WEP الذي يستخدم مفتاح واحد لجميع المستخدمين. وللإتمام عملية ال WPA يجب إدخال جميع الأرقام السرية في نقطة الوصول " Access Point". ويتكون هذا المفتاح من ١٢٨ بت ولكن بقيمة ابتدائية مكونة من ٤٨ بت مما يجعل WPAأقوى.

من ناحية الاختراق. كما نلاحظ أن هذا الطول مساوي للمفتاح في ال WEPمما يعني أنه ليس هناك اختلاف؟

الاختلاف هو في تغير المفتاح تلقائيا مما يعني أن مستخدم ال WPA لن يقوم باستخدام المفتاح لفترة طويلة وهنا تكمن متانة هذا النظام.

لا يوجد نظام متكامل مما يعني أن هناك بعض العيوب التي ترافق ال WPA وهي:

-ما تزال تعتمد على المفتاح الذي يمكن التقاطه في حين الإرسال ومن ثم استخدام الاختراق المعجمي "Attack dictionary" للحصول على الرقم السري.

-قد يعاني من توقف الخدمة DoS وذلك إذا أدخلت كلمة المرور أكثر من مرة بطريقة غير صحيحة سيتم حجب المستخدم عن الدخول إلى الشبكة اللاسلكية.

أخطار أمنية محتملة على الشبكات اللاسلكية

- اتصال أشخاص غير مصرحين بالإشارات اللاسلكية و بالتالي الاتصال بالشبكة اللاسلكية ككل.
- بإمكان المخربين من التقاط و قراءة البيانات المرسلة على الهواء.
- بإمكان الموظفين من تركيب شبكات لاسلكية في مكاتبهم و بالتالي خرق قوانين حماية الشبكة في منظماتهم.
- يمكن للمخربين من اختراق الشبكات اللاسلكية بسهولة بواسطة برامج اختراق بدائية جاهزة.
- حرب *الشوارع* و هو مصطلح للتعبير عن التجوال بغرض اكتشاف و اختراق شبكات لاسلكية غير محمية.

نصائح لحماية الشبكات اللاسلكية

- تغيير اسم المستخدم و كلمة المرور الابتدائية لنقطة الاتصال و الموَجه ، وذلك لمنع الأشخاص الغير مصرح لهم من الاتصال بالشبكة بمجرد لتخمين اسم المستخدم و كلمة المرور الموضوعة ابتدائيا من قبل الشركة المصنعة.
- تنشيط خاصية التشفير ، وذلك لمنع الأشخاص الغير مصرح لهم من التقاط الإشارات و بالتالي التعرف على البيانات المرسلة.
- تغيير اسم الشبكة الابتدائي ، لمنع معرفة اسم الشبكة بمجرد التخمين بالاسم الموضوع من قبل الشركة المصنعة.

- تنشيط خاصية فلتره العناوين للأجهزة المتصلة بالشبكة، لقصر الاتصال فقط على عناوين معروفة مسبقا ومنع الاتصال للعناوين الغير معروفة.
- إلغاء خاصية نشر اسم الشبكة (SSID)، لمنع اكتشافها و قصر الاتصال على من يعرف اسم الشبكة اللاسلكية.
- تحديد عناوين انترنت (IP) ثابتة للأجهزة في الشبكة اللاسلكية ، و بالتالي سيساعد ذلك على عملية التشفير للعناوين (IPs).
- تحديد مكان مناسب لنقطة الاتصال و المَوجه من حيث مدى انتشار الإشارات اللاسلكية ، و أنها تكون قدر الإمكان داخل منطقة آمنة .
- تركيب جدار ناري (Firewall) لمنع الاتصال الغير مصرح و لإخفاء الشبكة.
- التحديث المستمر للبرامج المشغلة لمكونات الشبكة (نقط الاتصال ، الموجهات ،...) عن طريق الشركات المصنعة.
- متابعة أخبار الشبكات و خاصة الشبكات اللاسلكية في مجال الأمن و تطبيق التحديثات و الأنظمة الأمنية الجديدة.

الخاتمة

أحدثت الشبكات اللاسلكية تغير وتطور كبيرين في استخدام و بناء الشبكات و طريقة الاتصال بها أيضا ، و و اكب هذا التغير اهتمام متزايد بأنظمة الحماية لهذا النوع من الشبكات التي بطبيعتها نظرا للتراسل على الهواء عرضة أكبر للتهديدات الأمنية ولذلك يجب الاهتمام بالجانب الأمني و التأكد من تطبيقه بالشكل الكافي و المحدث.

تم بعونه تعالى

Moustafa-MN@hotmail.com

- **Reference :**

- http://www.wi-fi.org/getfile.asp?f=WFA_02_27_05_WPA_WPA2_White_Paper.pdf
- http://telecom.gmu.edu/publications/Kieth-Fleming-Wireless-Security-Project-f2-May-2005.doc
- http://demo.ebusiness.uoc.gr/index.php?op=modload&modname=Downloads&action=downloadsview&pageid=1513
- http://www.invictusnetworks.com/faq/Securing%20Wireless%20LAN/Wi-Fi_ProtectedAccessWebcast_2003.pdf
- http://www.wi-fi.org/getfile.asp?f=Whitepaper_Wi-Fi_Security4-29-03.pdf